Remarks:

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1–31 remain in the application. Claims 8, 17 and 19 are amended. Claim 8 is amended to correct a grammatical error only. Claims 24-31 are added to recite further embodiments of the invention, as would be understood by one of skill in the art in accordance with the specification as originally filed.

ARGUMENT

The objection to Claim 19 is moot based on the above amendment.

Claim 17 is rejected under 35 U.S.C. § 112, second paragraph. This rejection is moot based on the above amendment. Claim 17 is amended to recite the state of a feature of a system resource rather than *optional feature* to be consistent with the wording of the claim.

Claims 1-4, 8-14 and 17-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,463,537 to Tello (hereinafter, "Tello"). This rejection is respectfully traversed and Claims 1-4, 8-14 and 17-20 are believed allowable based on the above amendments and following discussion.

With regard to Claims 1, 8 and 17, the Examiner asserts that Tello teaches *receiving, at a BIOS, a message from an authorized party; authenticating the message; and controlling a state of a feature of a system resource, using the BIOS, according to the message.* The claims further require that *the message comprises information to determine the optional feature* or *state of a feature of a system resource.* Tello teaches that a personalized computer with a unique encrypted digital signature will not boot up or recognize any data storage or communication peripheral devices without a matching personalized smartcard containing a complementary encrypted digital signature. The smartcard contains an authenticating identifier. Further, the system includes a security engine microprocessor and a modified BIOS (Basic Input Output System) that replaces the standard BIOS of a motherboard and allows the security engine microprocessor to take over pre-boot control of the computer from the motherboard CPU. The system of Tello matches the identifier in the smartcard with the security system. Communication is synchronized between the

inserted smartcard and the security engine microprocessor as occurs every time a smartcard is inserted in the smartcard reader. Tello does not teach or suggest a method to adapt a system during run-time based on data in the smartcard.

Tello teaches that the smartcard reader is connected to the security engine microprocessor. A software program in the flash memory of the security engine compares the hash numbers in the smartcard and the computer. Next, hash numbers are read from the smartcard the hash numbers are read from the security engine flash memory. The smartcard hash numbers are then compared to the security engine's hash numbers. If the hash numbers in the smartcard and security engine memories do match, the security engine microprocessor reads the security configuration parameters from the flash memory and all allowed peripheral devices are enabled.

In contrast, the claimed invention relates to enabling optional features on a computer based on authorized ***messages*** received ***by the system BIOS***. The claimed invention does not require a second microprocessor in the system to read security information from a smartcard. The claimed invention is a system and method for authorizing and enabling *optional* features of the system based on messages received at the system BIOS. The recited invention requires the receipt of a message, where the message defines the optional parameters. Tello does not teach or suggest that the BIOS receives messages or any communication from an authorized party. Tello teaches that a smartcard is used to decrypt and authenticate a digital signature which allows a computer to boot. Moreover, the system, as taught by Tello, does not receive a message at the BIOS. This distinction was overlooked by the Examiner. Instead, the security engine microprocessor of Tello reads hash numbers from the smartcard. There is no direct connection or communication between the messages and the system BIOS. Further, once there is a match, the information defining the allowed peripherals is read from the flash memory of the second microprocessor (security engine), not from the incoming message. Also, if the smartcard is not present, Tello's system will fail to boot. Applicant's claimed invention does not preclude booting in a default state. One of ordinary skill in the art will recognize that when *optional features* of the system resources are not authorized, or unverified messages are discarded, that **non-optional** features will still boot normally.

Applying the teachings of Tello to the present invention would require a smartcard reader and a security engine microprocessor. Applicant's claimed invention may have advantages to the teachings of Tello in that it does not require additional hardware or processors to operate. Further, applying Tello to the present invention would prohibit the system from booting when a message is not received by the BIOS. It will be apparent to one of ordinary skill in the art that the techniques used to secure a system and/or data from unauthorized users (Tello) or prevent booting are not the same as for a system which allows dynamic updates to the system features to activate, inactivate or modify parameters of system resources (present invention).

The Examiner asserts that Tello teaches that the message *comprises information to determine the optional feature, and wherein the message further comprises a digital signature.* Tello does not teach messages are received by the BIOS. Tello teaches a software program in the flash memory of the security engine microprocessor compares the hash code in the smartcard to a hash code in the computer. If the numbers match or are complements, "the boot up procedure is allowed to continue." [Col. 5, line 32] Thus, Tello teaches away from the claimed invention. Tello does not teach that *optional features* may be enabled, but only that a microprocessor and smartcard may supersede normal boot up procedures of a system BIOS and cause a halt in pre-boot operations. Further, the reference cited by the Examiner (Col. 31, lines 29-60) does not teach or suggest that a message *from an authorized party* is received at the BIOS. The flash memory of the security engine is part of the system. One of ordinary skill in the art would understand that an *authorized party* means a message from an OEM or similar, not data encoded in the system. "The secure environment guarantees authenticity, privacy, and validation of messages from the OEM. The secure environment assures that a message from the OEM for enabling system features will be received and processed in a secure manner." (Specification, page 5).

Thus, Tello fails to teach or suggest all of the recited elements of Applicant's invention and Claims 1, 8, 17 and their progeny are believed allowable.

As for Claims 2, 11-12 and 18, the Examiner asserts that Tello teaches v*erifying an identifier in the message against a unique system identifier of the system.* Tello teaches identifying the purpose and type of the smartcard. Tello does not teach or suggest a unique system identifier, and further, does not teach or suggest a message having an identifier to

compare to the unique system identifier. Tello does not teach any message communication, but merely reading data in the smartcard and application of the data to authorize boot and data access. Specifically described at the cited reference, Tello teaches that the flash memory of the microprocessor has a secret identifier. However, Tello teaches that the identifier is 'the same for all motherboards." [Col. 9, lines 20-30] This argument was promoted because the Examiner misunderstands the implication of a single unique system identifier. Tello does not teach a system identifier. Tello teaches that each smartcard has a unique hash number or digital signature. Upon security setup, a complementary hash number is stored in the security engine microprocessor memory. Since Tello teaches a system that may be used by many users, each with their own smartcard, the security engine microprocessor may have many complementary hash codes stored for as many authorized smartcards. Further, a user may be authorized to use more than one system. Thus, the unique hash number is associated with the smartcard and many systems may contain its complementary hash number to allow the user to boot each system. Thus, Tello teaches away from a "***unique system identifier of the system***" as recited in Claims 2, 11-12 and 18, and merely teaches a unique hash number associated with a smartcard. Moreover, with respect to claim 11, Tello does not teach a write-once non-volatile unit for storing a unique system identifier *accessible by the BIOS*. Thus, Claims 2, 11-12, 18 and their progeny are believed allowable.

As for Claims 9-10, the Examiner asserts that Tello teaches *a write-once non-volatile unit for storing a public key accessible by the BIOS*, citing Col. 15, lines 6-13. Tello teaches a smartcard with a ROM that contains six encryption keys, also stored on flash memory in the security engine microprocessor. First, this flash memory is not accessible to the system BIOS, but only accessible to the security engine microprocessor. Applicant's claimed invention does not require a second processor with an engine taking over for the BIOS. Second, flash memory is not write-once memory, but as will be apparent to one of skill in the art, may be written over many times. Third, the ROM on the smartcard is also not accessible to the BIOS for the same reasons that the flash memory is not. Thus, Claims 9-10 and their progeny are believed allowable.

As for Claim 13 and 14, Tello does not teach or suggest *a secure non-volatile location for storing at least one of the optional features to be enabled, the location being readable and*

writable by the BIOS. As discussed previously, Tello teaches that only the security engine microprocessor has access to the smartcard and its data, not the BIOS. Further, Tello does not teach enabling optional features, but teach whether the system should boot at all. While Tello describes that messages may be sent to the BIOS during setup and generation of boot subroutines, Tello does not teach that the non-volatile location for storing optional features is readable and writable by the BIOS. Tello teaches storing information in the smartcard and in locations accessible and writable by the security engine microprocessor.

Claims 3-4 and 19-20 are believed allowable as being based on allowable base claim. Further, the Applicant maintains that Tello does not teach the writing of messages.

Claims 5 and 21 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No.6,581,159 to Nevis et al. (hereinafter, "Nevis et al.). This rejection is respectfully traversed and Claims 5 and 21 are believed allowable based on the foregoing and following discussion.

Without conceding the propriety of combining these references, Applicant respectfully submits that Nevis et al. cannot be used as a reference to render the present invention unpatentable. More specifically, Applicant respectfully points out that Nevis et al. is co-owned by the assignee of the present application. As articulated in 35 U.S.C. 103(c):

> "Subject matter developed by another person, which qualifies as prior art only under one or more of subsections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the claimed invention was made, owned by the same person or subject to an obligation of assignment to the same person"

Since Nevis et al. does not qualify as a reference under 35 U.S.C. 102 (a), (b), (c) or (d), it may only be deemed prior art under 35 U.S. C. §102 (e), (f) or (g). As a result, pursuant to 35 U.S.C. §103(c), Applicant respectfully submits that Nevis et al. does not preclude patentability of the presently claimed invention since Nevis et al. and the presently claimed invention were, at the time the claimed invention was made, owned by the same person or subject to an obligation of assignment to the same person. More specifically, Nevis et al., which issued on June 17, 2003 as U.S. Patent No. 6,581,159, is assigned to Intel Corporation, the same entity to which the current application is assigned (assignment recorded on Oct. 1, 2001). As such, Applicant respectfully

submits that Nevis et al. is an improper reference for use against the presently claimed invention and Applicant requests the Examiner to withdraw the rejection to Claims 5 and 21 under 35 U.S.C. §103.

Claims 6, 16 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No.6,704,789 to Ala-Laurila et al. (hereinafter, "Ala-Laurila et al.). This rejection is respectfully traversed and Claims 6, 16 and 22 are believed allowable based on the foregoing and following discussion.

Claims 6, 16 and 22 are believed allowable as being based on allowable base claims, as discussed above. Ala-Laurila et al. teach a method of providing a user a terminal network address in a first network through which the user communicates with a data network and authenticating connection of the user to the first network. The authentication mechanism in a first embodiment utilizes a user identification stored in a second network providing connectivity between the user and the first network which may be obtained from a smartcard in the user terminal. Alternatively, in second and third embodiment taught, the authentication mechanism uses a user identification stored in the first network. This method is similar to the system and method taught by Tello. Both system and methods are directed toward authorizing users on a system. In contrast, Applicant's claimed invention requires using the BIOS to authenticate a message to control optional features. Who the user of the system is not particularly relevant. Authorization is by system not user. In particular, Claims 6, 16, and 22 use the BIOS to load and execute the message at runtime, wherein the message is received via a network transmission. Neither Tello or Ala-Laurila et al. teach or suggest executing content of the message at run-time, wherein the message is received via a network transmission. Tello, for instance, does its authentication during pre-boot only in order to decide whether to continue booting the computer at all. Further, a combination of Tello and Ala-Laurila is improper as Tello teaches that a smartcard must be inserted into the system to authenticate a user. Tello's system either would not operate, or would teach away from Applicant's claim invention if network transmission as taught by Ala-Laurila et al. was used. The smartcard is shown connected to the smartcard interface which is connected to the security engine microprocessor. (See Fig. 1) Specifically, it is taught that:

> "The programming circuit 129 is logically connected to the security engine microprocessor 123, the security engine scratch memory 127, and the smartcard reader 133 through the smartcard interface 135. The smartcard interface 135 is shown in FIG. 2 and is comprised of PA0136, PB0138, PB1140, PB2142, PB3149 and Reset 150 lines which have pull down resistors on them, and Clock 152, Ground 154, and (Supply voltage) VCC 156 lines." [Col. 6, lines 60 et seq.]

As taught, the security engine microprocessor is connected to the local bus to the PCI bridge [Fig. 1]. Modifying Tello with the teachings of Ala-Laurila et al. is not possible. It would not be possible to apply a network transmission to the use of the smartcard as taught by Tello. Thus, Claims 6, 16 and 22 are believed allowable.

Claims 7, 15 and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pub. No. 2001/0025312 to Obata (hereinafter, "Obata"). This rejection is respectfully traversed and Claims 5 and 21 are believed allowable based on the foregoing and following discussion.

Claims 7, 15 and 23 are believed allowable as being dependent on allowable base claims. All claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1 to 31 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 3 Nov. 2005

s/ Joni D. Stutman-Horn /

Joni D. Stutman-Horn
Patent Attorney
Intel Corporation
Registration No. 42,173
(703) 633-6845

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026